EUROPEAN DATA PROTECTION SUPERVISOR

PRESS RELEASE

EDPS/2013/08

Brussels, 19 July 2013

Smart borders: key proposal is costly, unproven and intrusive

There is **no clear evidence** that the Commission Proposals to create a **smart border** system for the external borders of the EU will fulfil the aims that it has set out, said the European Data Protection Supervisor (EDPS) today. Following the publication of his opinion which focuses specifically on the **Entry/Exit System**, the EDPS said that one of the stated aims of the proposals was to replace the existing 'slow and unreliable' system but the Commission's own assessments do not indicate that the alternative will be sufficiently efficient to **justify** the **expense** and **intrusions into privacy**.

Peter Hustinx, EDPS, said: "*Improving the management of border controls is a legitimate exercise. But it would be **more effective** to do this once a clear European policy on the management of over stayers has been established. In the absence of such a policy, the creation of yet another large-scale IT database to store massive amounts of personal information is a **disproportionate** response to a problem that other recently created systems may be able to help solve. It would be **prudent** both economically and practically to evaluate the **existing** systems at least to ensure **consistency** and **best practice**."*

The proposed Entry/Exit System relies on the use of **biometrics**, specifically 10 fingerprints, to verify the identity of individuals at borders in order to calculate the duration of the stay of third country residents. In a **democratic society**, the EDPS questions the **necessity** of the collection and storage of **excessive** amounts of personal information, particularly when two or four fingerprints are sufficient for verification.

As law enforcement authorities may potentially be granted access to the database after a period of evaluation of the system coming into force, it appears that the proposals are **anticipating** such access before demonstrating that the **intrusion** into the private lives of individuals is actually necessary. The **general trend** to give law enforcement authorities access to the data of individuals, who in principle are not suspected of committing any crime, is a **dangerous** one. The EDPS strongly recommends that the precise **added value** of such access, compared with access to existing biometric databases, be **identified**.

The EDPS urges that specific attention also needs to be paid to the **legal consequences** of **automating** border procedures. For example, the system will automatically calculate the length of stay of a visitor but the avoidance of mistakes through automation - for example, failure to register the exit of an individual because he is undergoing medical treatment or because of technical problems of the system - has not properly been addressed. Individuals must be fully informed in due time of any unfavourable decision taken against them so that they are able to exercise their rights. This is all the more **urgent** since the **multiplication** of databases in border management (such as VIS, SIS, CIS, EURODAC) makes it increasingly **complicated** for individuals to exercise their **rights**.

The routine functioning of the system will imply a need to **exchange** personal information with third countries in relation to the return of individuals. The EDPS recommends that the **specific** conditions and purposes under which those countries may be granted proof of the identity of their nationals needs to be substantiated, all the more important as many third countries do not offer the same **level** of data protection as is offered in the **EU**.

Background information

On 28 February 2013, the Commission adopted:

- a proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union
- a proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme (RTP)
- a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP).

On the same day, the proposals were sent to the EDPS for consultation. The EDPS had previously given his informal comments to the Commission before the adoption of the proposals.

Privacy and data protection are fundamental rights in the EU. Under the Data Protection **Regulation (EC) No 45/2001**, one of the duties of the EDPS is to advise the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues that have an impact on data protection. Furthermore, EU institutions and bodies processing personal data presenting specific risks to the rights and freedoms of individuals ('data subjects') are subject to prior-checking by the EDPS. If in the opinion of the EDPS, the notified processing may involve a breach of any provision of the Regulation, he shall make proposals to avoid such a breach.

Personal information or data: any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, e-mail addresses and telephone numbers. Other details such as health data, data used for evaluation purposes and traffic data on the use of telephone, email or internet are also considered personal data.

Privacy: the right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).

Privacy by design: to build privacy and data protection into the design and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.

Purpose limitation: personal information may only be collected for specified, explicit and legitimate purposes. Once it is collected, it may not be further processed in a way that is incompatible with those purposes. The principle is designed to protect individuals by limiting the use of their information to pre-defined purposes, except under strict conditions and with appropriate safeguards.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy;
- cooperating with similar authorities to ensure consistent data protection.